Union Calendar No. 3

100TH CONGRESS
1st Session

HOUSE OF REPRESENTATIVES

REPORT
100-5

UNITED STATES COUNTERINTELLIGENCE AND SECURITY CONCERNS—1986

REPORT

BY THE

PERMANENT SELECT COMMITTEE ON INTELLIGENCE HOUSE OF REPRESENTATIVES

FEBRUARY 4, 1987.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

---

U.S. GOVERNMENT PRINTING OFFICE

68-440 WASHINGTON : 1987

Union Calendar No. 3

100TH CONGRESS *1st Session* | HOUSE OF REPRESENTATIVES | REPORT 100-5

UNITED STATES COUNTERINTELLIGENCE AND SECURITY CONCERNS—1986

FEBRUARY 4, 1987.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. STOKES, from the Permanent Select Committee on Intelligence, submitted the following

REPORT

EXECUTIVE SUMMARY

Over the past several years, a dangerous upward trend in successful espionage operations against the United States has occurred. Present and former U.S. Government employees with access to sensitive classified information have played the key roles in each operation. Damage to U.S. national security has been significant and is still being estimated.

Deeply concerned over these developments, the House Permanent Select Committee on Intelligence has spent a great deal of time investigating this alarming situation. This report represents one outcome of the investigation.

From its early days, the Administration has focused considerable attention and effort on improving the effectiveness of U.S. counterintelligence. Concomitantly, the House and Senate Intelligence Committees have authorized significantly increased funding for counterintelligence and urged that counterintelligence concerns assume a higher priority within the Intelligence Community. These efforts have elevated the morale, status and numbers of counterintelligence personnel, helped cope with security investigation backlogs and encouraged new initiatives in some operational and policy areas. Nonetheless, it has become apparent that historical inadequacies in counterintelligence and countermeasures are so deep-seated and pervasive that fundamental problems remain. These must be addressed now with renewed determination and vigor.

From its hearings and interviews, the Committee has determined that serious security deficiencies exist in a number of areas within

the U.S. intelligence community. These deficiencies include faulty hiring practices, inadequate and inefficient background investigations, lack of full coordination and information exchange between agencies, insufficient adherence to the "need-to-know" principle, over-classification of security documents and proliferation of personnel clearances, thoughtless firing practices, and over-classification of security documents and proliferation of personnel clearances, thoughtless firing practices, and over-reliance on polygraph exams.

The Committee recognizes that the intelligence community has acknowledged some of the problems addressed in this report and that some of the solutions suggested herein already are being implemented. The Committee applauds these efforts, but urges still greater attention to counterintelligence issues, beginning with acknowledgment that manifest failures have reflected systemic inadequacies rather than mere aberrations or unavoidable risks. In general, within the intelligence community there appears to remain insufficient appreciation for the importance of counterintelligence concerns, an attitude often reflected in internal agency budgetary and policy prioritizations. Moreover, despite some recent improvement, the fragmented components of the counterintelligence community remain uncoordinated, divided and turf-conscious in virtually every substantive area, ranging from simple information-sharing or investigation to policy formulation and counterintelligence operations. Dramatic improvement will require fundamental shifts in attitudes as well as in approaches and practices. This report concentrates almost exclusively on personnel and other security issues, but the adequacy and effectiveness of U.S. Government efforts in other counterintelligence areas should be re-examined as well.

The Committee urges the Director of Central Intelligence and other key officials within the intelligence community to undertake all possible measures, beginning with those suggested in this report, to correct these deficiencies and to raise the level of vigilance against hostile espionage activity.

The Committee further stands ready to facilitate and to support appropriate remedial actions in this vital area.

SUMMARY OF FINDINGS AND RECOMMENDATIONS

The Committee makes the following key findings:

(1) Security weaknesses represent a serious management failure in the U.S. intelligence community.

(2) Weaknesses in the process of selecting personnel for initial employment in U.S. intelligence agencies constitute a key threat to national security.

(3) Senior managers of U.S. intelligence agencies have downplayed the seriousness of counterintelligence and security failures and have not taken adequate measures to correct deficiencies.

(4) The polygraph is a useful tool in security screening of personnel, but the U.S. intelligence community places excessive reliance on the value of the polygraph interview.

(5) The attitude prevalent among intelligence community personnel that those who have "passed" a polygraph interview are an elite of unquestionably loyal employees with respect to whom secu-

rity precautions may be relaxed is dangerous, especially in light of recent espionage cases in which foreign spies successfully "passed" CIA polygraph interviews.

(6) No adequate mechanism exists within the government for ensuring that information of counterintelligence and security value possessed by one intelligence agency is available to other intelligence agencies which would benefit from it.

(7) The potentially most damaging long-term development in classified information security practices is erosion of the principle that access to classified information requires not only the requisite clearances and special access approval, but also a need to know the information to perform official duties.

(8) Too many clearances are granted.

(9) Too much information is classified that would not reasonably cause damage to the national security.

(10) Superficial background investigations often do not discover alcohol, drugs, and financial problems.

(11) No focal point exists within the government for centralized storage, retrieval, and dissemination of background investigation information.

(12) Financial pressure, not ideology, constituted the primary motivation of many spies apprehended in the United States in recent years.

(13) In several recent espionage cases, intelligence agency employees satisfied security standards at the time of employment, but after employment decided to engage in espionage, and never were subject to routine security reinvestigation after employment.

(14) Former employees of intelligence agencies who had access to sensitive secrets may pose as potentially great a risk to security as current employees with such access.

(15) Other than the intelligence committees of the House and the Senate, the Congress has no personnel, physical, document and communications security programs which meet or exceed all applicable executive branch security standards.

(16) Dangerous laxity exists in the communications and computer security practices of many federal agencies.

The Committee makes the following key recommendations:

(1) U.S. intelligence agencies should undertake a coordinated review of their hiring practices.

(2) The President should authorize an independent group of experts outside the intelligence community to examine thoroughly the damage to U.S. intelligence capabilities resulting from recent espionage cases and to urge needed adjustment of U.S. intelligence collection techniques.

(3) All U.S. intelligence agencies should be required to report as appropriate to the Director of the Federal Bureau of Investigation or the Director of Central Intelligence information they possess which raises a suspicion of possible espionage.

(4) U.S. intelligence agencies should institute a rigorous need-to-know policy to govern access to classified information and back that policy by disciplinary action against employees who breach that policy.

(5) The Director of Central Intelligence should consider establishing a system for dissemination of intelligence with minimal source

identification, restricting full knowledge of sources only to those who absolutely need to know.

(6) The executive branch and the Congress should work to standardize, expedite, and adequately fund the security clearance process. The Secretary of Defense, in consultation with the Director of Central Intelligence, should examine whether the Defense Investigative Service (DIS) can serve adequately the personnel security background investigation needs of the military departments and defense agencies and should consider whether such departments and agencies should undertake their own background investigations and whether they should contract with private firms for such investigations. The Congress should carefully examine the budget request for DIA within the FY 1988 Defense budget review process.

(7) Background investigations should focus more on the financial status of the subjects of the investigations.

(8) Periodic reinvestigation of personnel with access to sensitive compartmented information, i.e. the nation's most sensitive intelligence secrets, should be given priority equal to that of initial investigations.

(9) Legal and administrative mechanisms should be established to ensure that agencies which possess information of security relevance on an employee or applicant for employment of another agency share that information with that agency.

(10) The National Security Council, the Attorney General, the Secretary of Defense, and the Director of Central Intelligence should review jointly executive branch policy with respect to former government personnel and personnel of government contractors who has access to sensitive compartmented information and consider changes, such as requiring exit interviews and a separation non-disclosure agreement, to deter post-employment unauthorized disclosures of classified information.

(11) The leadership of the House of Representatives should examine the feasibility of establishing uniforms security procedures for House committees, offices and organizations which meet or exceed executive branch standards.

(12) The Federal Bureau of Investigation should establish a program of rewards for information leading to the arrest of individuals for espionage.

(13) Strict, rigidly applied communications and computer security practices should be established within the U.S. Government.

(14) The Attorney General, the Director of the Federal Bureau of Investigation and the Director of Central Intelligence should consider realigning some FBI surveillance resources to high priority intelligence targets. The Congress should carefully weigh the amount of resources requested for this purpose in the FY 1988 budget review process.

INTRODUCTION

From 1984 to 1986, twenty-seven U.S. citizens were charged with espionage. To date, all but one (Craig Smith) who have been brought to trial have been convicted. Among this number were naval officers John and Arthur Walker, John's son Michael and friend Jerry Whitworth, both sailors; naval intelligence analyst

Jonathan Pollard; FBI agent Richard Miller; ex-NSA specialist Ronald Felton; CIA analyst Larry Wu Tai Chin; and CIA secretary Sharon Scranage. Never apprehended was fugitive ex-CIA officer Edward Howard, who is now in Moscow.

These examples of espionage did not occur in a vacuum. The Committee receives regular reporting from the intelligence community concerning the vigorous, well-financed and widespread efforts of the Soviet Union and its communist allies to steal U.S. national security information. The occasional arrest of diplomats, United Nations employees and foreign commercial representatives reveals only the tip of the iceberg of foreign espionage. That espionage efforts are highly productive for hostile foreign nations can be seen in the sometimes startling technological advances in Soviet weaponry and in the compromise of formerly productive U.S. intelligence operations.

Against this background of pervasive espionage, the question raised by the espionage cases reviewed by the Committee, all of which directly concerned the compromise of codes or intelligence activities, was whether the U.S. intelligence community and the larger national security community maintained adequate security. Were the individual involved in these cases—trusted, fully cleared, some with years of experience or high marks for performance—indicative of systemic flaws? Are there others like them and, if so, how could they be detected? How carefully did responsible government officials answer these questions and how vigorously did they pursue necessary remedies?

The following espionage cases were but a few examined by the Committee and reveal staggering, long term damage to national security:

—During a 15-year period, John Walker provided the Soviets with code cards and the plans to code machines used widely by the Navy. The Soviets undoubtedly read many of the classified messages concerning submarine movements and tactics sent using these machines during that period.

—Jerry Whitworth also provided other code cards and code machine plans that allowed the Soviets access to the same kind of messages both before and after Walker retired. He also provided copies of coded messages and other classified information about U.S. aircraft carriers.

—For two years, Jonathan Pollard provided thousands of highly classified intelligence reports to Israel, including reports the U.S. chose to share with no other country.

—Ronald Pelton, in a series of clandestine meetings with the Soviets in Washington and Vienna, provided detailed information on NSA's efforts at breaking Soviet codes and intercepting sensitive Soviet military communications. In those meetings, he gave the Soviets a good description of many U.S. signal intelligence capabilities against the Soviet Union and betrayed collection programs it had taken decades to establish.

—For 30 years, Larry Wu Tai Chin spied for China. During the last nine years of his career at CIA, he saw, and in turn gave to the Chinese, a great many classified CIA analyses about China.

—Sharon Scranage betrayed the identities of CIA agents in Ghana and perhaps in other African countries. Her disclosures crippled CIA capabilities in Ghana.
—Edward Howard betrayed the most sensitive operations of the United States in Moscow, which had a severe adverse impact on U.S. collection of intelligence in Moscow.

Most of the Americans who were caught spying between 1984 and 1986 had no ideological commitment to another foreign country. They sold U.S. secrets for financial reasons. Although some—like the Walkers, Whitworth and Chin—had exemplary careers, the behavior of others—Pollard, Miller, Scranage and Howard—offered warning signs to their superiors and co-workers. Often these problems were ignored or given insufficient attention by management. In the Jonathan Pollard case, co-workers' reports of his suspicious behavior led to apprehension and arrest.

SCOPE

The Committee has pursued the questions raised by recent espionage cases by examining the intelligence damage assessments on each spy, reviewing the investigations that led to each arrest, and studying carefully the conclusions drawn by executive branch officials and the changes undertaken to rectify problems identified. The Committee concentrated in its hearings, interviews and follow-up questions and answers on cases having particular relevance to the intelligence community. The conclusions drawn by the Committee thus apply to the intelligence community particularly, but clearly have relevance to the wider national security community, which is governed by many common security standards and practices. Although the Committee's examination has been limited in terms of the numbers of cases reviewed and the short time span, the implications of this representative sample are so disturbing that they demand review. Security is a critical aspect of every intelligence function. Intelligence operations by their nature must remain secret. Threats to that secrecy threaten the viability of a wide range of essential national security functions that are critically dependent upon intelligence.

FINDINGS AND RECOMMENDATIONS

Management

Overall, the Committee perceives a serious management failure in the U.S. intelligence community. Major flaws exist in implementing existing security procedures, including the granting of too many security clearances, improper document handling, violations of the need-to-know principle, poor supervision of personnel with access to classified information and a lack of coordination between agencies on security matters, to name but a few shortcomings. Underlying all of these problems has been a lack of either urgency or top priority at departmental and lower levels with respect to needed security changes, despite the high priority given to counterintelligence issues over recent years by the White House and by the Congressional intelligence committees. Once the glare of public scrutiny leaves the problems of espionage and security, the Committee is concerned that the political will to advance security pro-

grams and maintain high levels of attention and necessary funding for their implementation will not be sustained. The very size of the U.S. national security community, its complexity and lack of unitary management and the historically lower priority assigned to security concerns have produced cynicism and failure to change in the past and could once again.

Hiring

The committee has discovered a disturbing lack of judgment on the part of the U.S. intelligence community in its hiring practices. Jonathan Pollard was hired even though he had frequently boasted to friends that he was an agent of Israel's intelligence agency, the Mossad. He later engaged in espionage for Israel once he had gained employment with the U.S. intelligence community.

The CIA hired Edward Howard despite an extensive history of using hard drugs. This serious error was compounded when he was then given detailed information on several of U.S. intelligence's most sensitive collection operations before his probationary period had been completed (with accompanying polygraph). The information he provided the Soviet Union has severely damaged U.S. intelligence collection capabilities.

The CIA conducted its own investigation into this case. Yet, curiously, in its investigation, CIA management focused more attention and action (including reprimands) on the manner by which Howard was fired once management had discovered he was a problem and gave relatively little attention to how he was hired in the first place. The extent of Howard's drug use was underplayed in this review.

The Committee is disturbed that one CIA manager testified that no one was responsible for hiring Howard, that "the system" hired him. That is an unacceptable way to hire people who will have access to the nation's most sensitive intelligence secrets.

The Committee recommends that U.S. intelligence agencies undertake a coordinated review of their hiring practices. Senior management needs to take a serious look at why persons with a history of hard drug usage or with serious personality flaws have been hired in the past.

The Stillwell Commission and others have assumed that basic security screening procedures are adequate and that problems connected with background investigations can be resolved through better implementation of existing procedures and through increased manpower. This assumption is questionable. Given the large number of new cases to be processed, the sizable existing backlog and the requirements for additional reinvestigations, it is doubtful whether the current procedures can ever ensure more than a superficial background probe. Morever, it is uncertain whether existing criteria for risk assessment and selection are adequate. The intelligence community must search for methods that highlight those cases upon which to expend intensive efforts, that establish clearer criteria for acceptance or rejection and that minimize the man-hours expended on an average case while maximizing an investigation's quality. Examples of areas which appear to deserve more research attention include: more systematic and comprehensive research on the personalities, character and life-style of

past spies; how to apply this knowledge under present day standards of social conduct; computerization of some processing; and adaptation of personality-based profiling accepted in other social science disciplines as an element to be considered in the screening procees.

The Committee also urges management to focus more attention on separation from duty practices within the intelligence community. These practices could include in-depth exit interviewing. Such interviewing have proved highly beneficial in the private sector by identifying weaknesses in the organization not readily apparent to a supervisor in day-to-day operations and not likely to be volunteered by a serving employee.

Attitude

The Committee has found a puzzling, almost nonchalant attitude toward recent espionage cases on the part of some senior U.S. intelligence officials. The Committee understands that "there will always be spies" but the attitude of some officials toward these cases raises concern that significant security breaches are not being taken seriously.

As an example, the Committee was struck by the manner in which Navy officals underplayed the disclosure of the Walker spy ring in closed session before the Committee while other government officials publicly and more accurately described them as extremely grave. Similarly, the Committee has had difficulty obtaining from CIA officials clear statements and judgments about the damage caused by the Howard case. While the long term damage caused by Howard's disclosures may be difficult to gauge, certain damage must be assumed. Yet CIA officials have avoided enumerating such matters to the Committee.

A further concern of the Committee pertains to intelligence community use of the polygraph. Two spies employed by CIA—Karl Koecher, a Czech agent, and Larry Wu Tai Chin, a Chinese agent—took polygraph tests while they were spying for these countries but were not disqualified. Despite this knowledge, CIA officials have stated to the Committee that "quality control" problems caused this failure of the polygraph. The CIA and other intelligence agencies have used the polygraph in the past to detect other attempted espionage, but the Committee is very concerned that the present community attitude is not sufficiently critical of its present dependence on polygraph results. The Committee believes that the intelligence community needs to place additional emphasis on other means, such as background investigations, of checking the loyalty and trustworthiness of its employees, contractors, and others involved in intelligence activities. The Committee is puzzled by the lack of commitment of necessary resources to make clearly indicated improvements in the background investigation process.

Members of the Walker family spy ring betrayed key U.S. submarine technology. The technology led to improvements in Soviet submarines sooner than expected. These notable improvements in Sovet capabilities apparently were not considered as indicators of espionage. This lack of openness to the potential for espionage, or the related phenomenon of institutional overconfidence in U.S. advanced technology weapons such as submarines, leads the Commit-

tee to recommend that the DCI give greater emphasis to the comprehensive review of information concerning hostile foreign power activities.

The Committee does not believe that the U.S. intelligence community can go ahead on a business-as-usual basis in the wake of these espionage disasters.

Failure to coordinate

In two recent espionage cases, those of Edward Howard and Ronald Pelton, one intelligence agency failed to provide a timely alert of possible espionage. There is no way to know whether damage resulting from what was in fact serious espionage could have been avoided or at least mitigated had those agencies shared their concern with others, but it appears that some precautions could have been taken.

In one case involving a joint operation between two U.S. intelligence entities, one agency developed a concern that the operation has been compromised and conducted an investigation to try to determine whether or not this was correct. That agency did not inform the other agency involved in the operation of this concern. As it turned out, the operation had been exposed by a former employee of the second agency.

The Committee recommends that the heads of all departments, agencies and entities of the U.S. Government involved in intelligence and intelligence-related activities be required to report to the Attorney General and, as appropriate, to the Director of the FBI or to the Director of Central Intelligence, any suspicion they have of possible espionage.

Need to know

A relaxing of the "need-to-know" principle has occurred in recent years. There seems to be a widespread attitude within some U.S. intelligence agencies that once an employee has been granted a Top Secret clearance and has been cleared for access to Sensitive Compartmented Information (SCI), strict adherence to the "need-to-know" principle is not required.

The "need-to-know" principle, simply put, is that a person in authorized possession of classified information must determine that another person requires access to that information in order to perform a specific and authorized function and that such person has appropriate clearances and access approvals.

When security procedures are working properly, two distinct determinations must be made before those controlling classified information make it available to others. The first is that the prospective recipient has proper security clearances for access to such information. The second is that the recipient has a need for access to the specific information to perform official duties. Possession of a Top Secret clearance does not mean a person has a need to have access to any and all Top Secret documents.

A major tightening up of the "need-to-know" practice is in order. It is particularly disturbing to see the proliferation of detailed knowledge about intelligence sources and methods.

A technique called "compartmentation" was developed to establish certain restricted categories of information to which extremely

limited numbers of people would have authorized access. For example, when the U-2 reconnaissance aircraft was first built and put into use by the CIA, its very existence was known to a very few people. They were granted compartmented access. Others, even though they had Top Secret clearances, were not made privy to knowledge about the U-2.

Today, access to some "compartments" is granted to tens of thousands of cleared people. Clearly such "compartments" are virtually useless to protect sensitive information.

In some cases, access to compartmented source information has been expanded at an early stage in a technical intelligence collection system's development in order to gain as much support for it as possible while its bureaucratic sponsors fought for funding. For example, detailed knowledge of the capabilities of a proposed reconnaissance satellite was spread widely throughout the Departments of Defense and State when proponents were seeking support to build the system. A similarly casual attitude toward security helps explain why a manual explaining the operating characteristics of the satellite came so easily into the hands of CIA employee William Kamplies who sold it to the Soviets.

In several recent espionage cases, intelligence officials conducting damage assessments have told the Committee that they could only estimate what sensitive information had been compromised because they had no way of knowing what information the person guilty of espionage had gained access to beyond that for which he was specifically cleared. Edward Howard may have learned about extremely sensitive CIA activities for which he had no formal access by virtue of friendly conversation and overheard office discussion. Jonathan Pollard was able to gain access to large numbers of classified reports having no relevance to his responsibilities because he had unrestricted access to classified libraries. Apparently, Ronald Pelton learned the details of many signals intelligence activities despite having authorized access to only partial knowledge of those activities. The Committee also has noted instances in which intelligence community officials have violated their own compartmented practices by talking about sensitive operations in front of persons with no need to know.

Improved and enlarged automated information data bases have been made available in significant numbers to cleared intelligence personnel in recent years. The Pollard case revealed that anyone with an appropriate clearance and with access to a classified library could request and receive sensitive intelligence reports on subjects outside his or her area of legitimate interest.

In urging a renewed and reinvigorated application of the need-to-know principle, the Committee also wishes to warn against an attempt to restrict knowledge that is already widespread. Pretending that well-known information can be compartmented brings the whole compartmentation process into contempt.

The Committee understands and supports the concept of getting intelligence into the hands of those with a genuine need to know. In the case of the U.S. military, those with an officially validated need to know can number hundreds of thousands at any given moment. The Committee believes that such validations need to be periodically reviewed and vigorously questioned. In any event, the

Committee is convinced that the genuine needs of intelligence consumers can be met while doing a better job of protecting sources and methods.

The Committee recommends that departments and agencies which handle classified national security information institute a rigorous "need-to-know" policy for access to such information. by "rigorous" the Committee means that "need-to-know" principles must become reality rather than simply be paid lip service or be honored in the breach. This will require a serious reassessment of current practice. Once instituted, violations of agency "need-to-know" policies should constitute grounds for adverse personnel action, including dismissal.

Sources and methods

The National Security Act of 1947 assigns the Director of Central Intelligence responsibility "for protecting intelligence sources and methods from unauthorized disclosure." Successive Directors over the years have implemented procedures designed to protect intelligence sources and methods.

Espionage cases and leaks to the press which have disclosed sources and methods indicate the difficulty the Director faces in exercising that responsibility. There is an inherent conflict between the consumers of intelligence who want as much information as possible, including how the information was acquired, and the collectors of intelligence, who want to protect the source of the information. In addition, there is the normal inclination within any intelligence community element to boast, especially when competing for limited funds against other elements of the intelligence community, of intelligence collection successes. Finally, the budget process over the past fifteen years has produced an explosion of staffs within the executive branch with access to the entire range of sensitive intelligence collection efforts, as well as some increase in legislative branch staff.

One byproduct of this virtually institutionalized situation is that much sensitive source and method identification is inherent in the dissemination of intelligence information both within and outside the intelligence community. Source identification is not essential for many recipients, however, and even analytical elements often do not require the specificity they sometimes receive. This is not to say that analysts do not need to understand how reliable source material is, but that decisions to provide source material should be carefully, rather than automatically, made.

The Committee recommends that the Director of Central Intelligence devise a system whereby information collected by the intelligence community is sanitized and disseminated to those who need it without source identification. Only those who absolutely have to know the sources should have access to that information.

THE CLEARANCE PROCESS

Numbers of cleared persons

The sheer number of people with clearances presents an unmanageable problem for security. By 1985, over five million Americans (of which 1.5 million are in the private sector) held clearances for

access to classified information, a figure that represented an increase of 40 percent from 1980. Many thousands are added and subtracted each year. Certainly, there are millions of retired government employees and contractors who, although they no longer retain clearance, do retain knowledge of classified information. The chances of a few spies having received clearances among so many are high.

This is a serious management problem that has been highlighted more than once in recent years. Congress must address this huge number of clearances in concert with executive branch officials. Skepticism and systematic review should govern requests for clearances and the retention of existing ones.

With two exceptions (Koecher and Chin), the cases examined by the Committee showed that espionage occurred after those involved received authorized access to classified information. The challenge, then, is to keep the numbers of those who must be cleared as low as possible and develop better ways to screen potential spies. Although solutions will be difficult, these matters must be addressed.

There is also little evidence that the executive branch is willing to incur the cost of better security. Some increases in the number of investigations for security clearances have been requested in recent months, but thousands more would be required in order to do a thorough job on security clearances. The irony of this situation is that the United States has spent billions of dollars to acquire technologically advanced means of intelligence collection but seems unwilling to invest in the relatively few millions of dollars necessary to better protect them from compromise. This inherent inconsistency in management approach bespeaks an overemphasis on so-called "big ticket" programs to the detriment of support functions essential to their security from compromise. This imbalance hurts the continued effectiveness of U.S. intelligence.

Congress, for its part, has in past years cut back the number of Department of Defense investigators, thus contributing to the current problem. No one who has seriously reviewed U.S. security practices, however, should assume that doubling, or even tripling, the number of investigations will result in significant improvements in security. The daunting numbers of clearances and the large amount of classified information must be reduced before better security investigations can offer any real promise of improvement.

A number of recommendations to cut down on the number of people having clearances have been made in recent years by congressional committees and panels convened by the executive branch. The Committee believes it is vital to reduce the number of people who have access to certain sensitive types of information such as cryptographic material and intelligence sources and methods. An accross-the-board reduction in security clearances does not adequately address this problem. For example, reducing security clearances without adhering to a strict "need-to-know" policy is meaningless.

The Committee notes that the Department of Defense has begun to grapple with the task of cutting down on the number of personnel who are granted clearances. Since June 1985, the Department of Defense has reported a significant reduction in the numbers of

cleared persons and has downgraded the level of clearances held by others. That appears to be a commendable step in the right direction, but more needs to be done. Such a significant and rapid reduction, however, gives rise to speculation that the clearances that were eliminated or downgraded cannot have been essential.

Overclassification

The executive branch has not taken the necessary steps to reduce the amount of classified materials being produced. In 1984, 6,900 Federal officials with original classification authority classified 881,943 documents. Another 18.7 million documents were classified by derivative authority. In 1985, 7,014 Federal officials with original classification authority classified 830,641 documents. Another 21.5 million documents were classified by derivative authority. Some estimates of the number of classified documents in existence reach into the trillions. The Pentagon alone classifies 11 million new items each year. Controlling access to that enormous volume of material is an unmanageable problem.

According to a report recently prepared by Frederick M. Kaiser of the Congressional Research Service, Library of Congress, overclassification, that is, classification of information whose disclosure could not reasonably be expected to damage the national security:

—"strains limited protective resources and services by requiring more and higher levels of protection for information;

—"results in a more extensive, intensive, and costly personnel security system; the greater amount and higher levels of classified information require a greater number of initial security clearances, higher levels of clearances, and a greater number and more frequent reinvestigations;

—"imposes additional burdens on the declassification process simply by ensuring that more information needs to be screened for possible declassification;

—"aids those with access to unnecessarily classified information to gain access to appropriately classified information; and

—"damages the credibility of appropriately classified information and the integrity of the classification system; these developments have a threefold impact: they foster casual, if not "cavalier" (as some have charged), attitudes towards safeguarding classified information on the part of information managers and controllers as well as other personnel with access to national security secrets; they make unauthorized disclosures of any classified information less onerous for some employees; and they lessen public confidence in the system and harm its legitimacy."

The Information Security Oversight Office, in its FY 1984 Report to the President, described overclassification as a "threat to the credibility of the system." The Kaiser study also notes that "overclassification may unnecessarily limit the amount of information available to the scientific community and thus hinder national security that develops from scientific progress."

If the executive branch wishes to avoid congressional restructuring of the classification system, it must undertake initiatives to force those who classify to resist overclassification.

The Committee notes that, within the intelligence community at least, the development of newer and greater volumes of intelligence has created pressure for more classified information. Congress has approved the programs that lead to this information explosion while at the same time warning that better processing and reporting was essential to render this mass of collected data usable for the limited number of intelligence customers who need it. Ensuring that such information reaches those who need it in time to be useful has led to the hiring of more people to perform processing and analysis. One thing seems clear. However difficult it is to ensure the flow of useful intelligence to policymakers and military commanders while holding in check the numbers of people with security clearances, the dual problems of expansion of secrets and the numbers of those who know them will become worse in the future without coordinated security initiatives on a number of fronts.

Background investigation delays

The Department of Defense has the largest number of people with clearances. The process of clearing those people is gravely flawed.

In 1972, the Secretary of Defense created the Defense Investigative Service to carry out certain investigations, including background checks, previously performed by the military services and Defense agencies. It was perceived at the time that there would be significant financial savings in consolidating these investigative functions. What was not anticipated was that the huge increase in cleared U.S. Government personnel handling a great deal more classified documents would soon overload DIS's workforce. Neither Congress nor the executive branch has supported increases in manpower and funds to match this growth in demand for DIS investigations. The result has been an inevitable decline in the quality of such work.

The Committee has found dissatisfaction with the timeliness of the background investigations conducted by DIS. The National Security Agency, which once relied solely on DIS for some of its background investigations, several years ago requested additional personnel to augment its own background investigations capability so as not to have to rely on DIS.

An office within the Department of Defense with responsibility for collection of specialized foreign intelligence through reconnaissance contracted with a private firm to carry out its background investigations because of frustration with the time delays in DIS investigations.

The Committee recommends that the Secretary of Defense and the Director of Central Intelligence examine the question of whether the security background investigatory needs of the military services and the Defense intelligence agencies and entities can be adequately served by DIS. This study should explicitly address whether such elements would be better served either by performing in-house background investigations or by contracting for such investigations by private firms.

Background investigation quality

The quality of background investigations for security clearances is uneven and frequently inadequate. In 1984, approximately one percent of 200,000 requests for Top Secret clearances were denied. Problems associated with alcohol, drugs or finances sometimes go undetected due to the superficiality of background investigations. In part, this points out the need to improve the training and effectiveness of investigating agents as well as the need for more investigators. In part, it may also point up the need to review standards relied upon for background investigations as well as the consistency with which these standards are applied and the extent to which elements of an individual's personality or lifestyle, not individually disqualifying in themselves, are reviewed in making personnel decisions.

Need for more financial information

It is a sad fact that the preponderance of recent espionage cases have hinged on the greed of Americans willing to betray their country's secrets. In the Pelton and John Walker cases, information was available while these individuals were still employed by the U.S. Government (and in Walker's case, spying for the Soviet Union) that would have exposed serious financial difficulties. This information did not surface in background investigations or as a result of information derived from fellow employees or supervisors. In addition, former government employees such as Pelton who had access to important government secrets during their employment have experienced financial difficulties which may have led them to commit espionage.

The Committee notes that in the case of the Department of Defense, regulations setting forth the questions to be asked during a counterintelligence polygraph examination as part of a periodic reinvestigation do not address a person's financial situation other than to inquire as to whether or not cleared employees are in such difficult financial straits that they might become targets of foreign espionage.

The Committee is fully cognizant of the privacy interests of present and former U.S. Government employees and of the impact upon morale that the use of certain investigatory techniques would have but it believes strongly that financial information deserves a more important focus in background investigations. Background investigations and reinvestigations are critically incomplete—and security devisions based on them are equally flawed—absent essential financial information. Failure to consider such information in security investigations is a serious security flaw.

Need for Reinvestigation

In a number of espionage cases, for example those of Jonathan Pollard, Sharon Scranage, and Richard Miller, the individual who provided information to a foreign power successfully passed his preemployment background screening, and later had contact with the foreign intelligence service and offered to betray classified U.S. information. The Committee notes that in other recent espionage

cases (Chin, John Walker), the employees who engage in espionage were never subjects of reinvestigations.

The Committee believes periodic background reinvestigations should be required for every employee with access to classified information. Periodic reinvestigations should serve as a deterrent to anyone tempted to commit espionage. Government policy is to update compartmented intelligence clearances every five years but few agencies, both for manpower and financial reasons, have consistently implemented that policy. This is of particular and obvious concern for intelligence agencies. However, as in the case of security investigators, simply increasing the frequency of reinvestigations will be effective only in connection with significant reductions in the numbers of those requiring reinvestigation.

The Committee recommends that periodic security reinvestigations should be given the same priority as original background investigations and should be carried out especially for those with access to sensitive compartmented information. The Committee believes that the nation's long term goals should be the regular reinvestigation of all cleared employees and that necessary resources to achieve this goal must be required by the President and provided by the Congress.

The Committee recommends further that, during security investigations, particular attention should be paid to each individual's financial status. Clearly, not enough attention is uniformly paid to such information at present. For example, the FBI, which conducts background investigations of the Committee staff every five years, requests no information from staff concerning individual finances in conducting such investigations. The Committee has urged that such information be requested and reviewed. The FBI has thus far only agreed to review such information for Committee staff background investigations.

SECURITY-RELEVANT ADVERSE INFORMATION

Government departments and agencies are authorized but not required to share with one another adverse information developed about employees. If an employee of one agency applies for employment at another agency and a background security investigation is conducted, the agency where the individual is currently employed is authorized by Executive Order 10450 to share adverse information with the prospective employer. The Committee has found that agencies sometimes will fail to share such information in order to rid themselves painlessly of a problem employee. In the case of applicants who are turned down by one agency and apply to another, there is no requirement that adverse information turned up in the first agency's background investigation be shared with the second agency.

Further, there is no focal point within the executive branch for the centralized storage, retrieval or dissemination of background investigation information. An individual denied a clearance at one agency could obtain the same level of clearance from another agency without the second agency being aware of the basis of the first agency's action. The executive and legislative branches could

do much more to standardize, streamline and improve the monitoring of clearances.

A particularly unfortunate example of failure to share adverse information was the case of Edwin Wilson, who left CIA to work for naval intelligence. He was still working for the Navy when he began efforts to sell arms to Libya. He was later convicted of illegal arms shipments and attempted murder of a government prosecutor.

The Committee also found that the Navy granted Wilson a clearance and used him to run an intelligence proprietary (front company) even though the FBI had information that a hostile intelligence service knew of Wilson's prior CIA activities. No record exists of FBI notice to the Navy of this information.

The Committee is pleased to find that there is frequent cooperation between elements in the intelligence community in this regard, but the Committee has also been informed that this is not always the case. Apparently, concern over disclosing intelligence sources or operations has led to withholding adverse information on occasion. Earlier information about Edward Howard known to the CIA—such as the circumstances surrounding his dismissal, or his psychological problems—might have placed the FBI in a better position to detect Howard's espionage.

The Committee recommends that renewed attention be devoted to ensuring adverse information about employees moving from one agency or department is shared with the new agency as required by E.O. 10450. It ought to be possible both to alert another government agency to a problem with a prospective employee and to protect intelligence sources. The Committee recommends that the provisions in Executive Order 10450 requiring the sharing of information on current employees be extended to applicants for employment. Any statutory changes needed to effectuate these recommendations should be proposed to the Congress.

POLYGRAPH

The pros and cons of the polygraph as a security protection have been debated at great length. The Committee does not intend to join that debate in this report. The Committee does wish to make certain observations. however, concerning the use of polygraph exams by the U.S. intelligence community for security and counterintelligence purposes.

The Committee's first observation is that those who have "passed" a polygraph exam look upon themselves as having joined a set of elite government servants set apart from the rest of the federal workforce. Such an attitude has resulted in a lessening of attention to routine and common sense security procedures, such as "need to know," among those who have been polygraphed. The Committee wishes to reemphasize that a strict need-to-know policy should be practiced even among those who have been polygraphed.

Moreover, intelligence agency managers appear to have placed an inordinate degree of trust in the polygraph examiners' skills. That trust seems in no way shaken by the discovery that foreign intelligence agents were not disqualified by CIA polygraph tests.

The polygraph is a useful tool in the security clearance process. For instance, in the Howard case, it served to identify information that led to his dismissal. However, use of the polygraph is not and should not be considered a substitute for thorough background investigations or other security procedures.

Accommodating National Security and Privacy Interests

The polygraph cannot be viewed as more than a tool for investigations. It will produce false negative or false positive indications in some circumstances. Intelligence agencies must protect security and protect employees and applicants by limiting reliance on the polygraph and making appropriate use of other investigative techniques.

The Committee seeks an improved clearance process with fairness to employees and applicants. A mutual tension exists between necessary criteria for security adjudication and protection of the rights of each individual. No simple method will resolve this tension. Reasonable standards which realistically relate to loyalty and trustworthiness must be coupled with careful individual adjudication of difficult cases.

FORMER EMPLOYEES

In the Pelton, Howard, and Walker spy ring cases, former employees of the U.S. Government sold classified information to the Soviet Union. Both cases raise serious questions about the ability of intelligence agencies or the Department of Defense to monitor the conduct of people after they have left sensitive government employment.

There is a need to assure that people who have been granted access to classified information continue to protect that information even after they are no longer employed by the government. The Committee recommends that the National Security Council, the Secretary of Defense and the Director of Central Intelligence review jointly executive branch policy with respect to former government employees and contractors who had access to sensitive compartmented information and consider changes—including requiring all employees who receive security clearances to sign a non-disclosure agreement upon separation and to participate in thorough exit interviews—that could deter unauthorized disclosures by such individuals. In conducting this review, full consideration should be given to safeguarding the privacy of such persons as well as the potential impact of new policies on employee morale.

CONGRESSIONAL SECURITY

Whatever their shortcomings, the executive branch has systems for classifying information, for clearing personnel and for handling classified material. Congress has no comparable system. The Permanent Select Committee on Intelligence has a system which meets or exceeds all applicable executive branch standards, but its procedures apply only to the Committee. Yet there are hundreds of Congressional employees with security clearances, numerous committees that receive and store classified information, and a different security system for each committee or Congressional agency.

The implications of this situation are serious. Intelligence reports and previous espionage cases such as that of ex-CIA officer David Barnett show that Congressmen, Congressional committees, and Congressional staff are potential targets of intelligence gathering by foreign countries. For example, Barnett was instructed by the Soviets to apply for a staff position at one of the Congressional intelligence committees. Electronic listening devices have been discovered in the past concealed in one House committee hearing room. In view of such efforts by foreign intelligence services, the disorganized and varying practices of Congressional offices and committees for handling classified information play into the hands of potential espionage efforts.

The Committee recommends that the leadership of the House examine the feasibility of establishing uniform security procedures for all House committees, offices and organizations which compare favorably with, and improve upon where possible, those of the executive branch. Such a study, to be comprehensive, should be based on a survey of House security practices. Further, the House should be prepared to devote the necessary resources to thoroughly address security needs.

DEFECTORS

As the well publicized case of defector Vitaly Yurchenko demonstrates, the intelligence community has experienced difficulty in handling some defectors. In part this has resulted from the high expectations and inflexibility of defectors themselves. As difficult as handling defectors may be, it is also crucially important to the national security.

The Committee believes higher priority for the program and more compassion for defector's needs should be devoted to the defector handling process. Some improvements have been undertaken in the wake of the Yurchenko case. The Committee believes that even incremental improvements in these areas could be of enormous importance in the retention of key defectors and their disclosure of foreign espionage activities.

COMMUNICATIONS SECURITY

The discovery that the Walker-Whitworth espionage ring provided the Soviets with the ability to decode U.S. Naval communications dealt a serious blow to the national security. The Committee has found appalling those communications security lapses that made the wholesale theft of cryptographic materials by John Walker and Jerry whitworth possible.

Further, senior U.S. Government officials often are careless about how they use car telephones. Sensitive matters also have been discussed on non-secure communications by senior Administration officials communicating with Air Force One. Apparently, Drug Enforcement Administration personnel in overseas posts frequently use open telephone lines to discuss anti-narcotics activity, in open disregard for vigorous and successful communications intercept efforts aimed at local, state and federal anti-narcotics agencies by international narcotics traffickers. The final go-ahead request for Navy aircraft to force down the Egyptian airliner carry-

ing the Achille Lauro terrorists was phoned in the open to Air Force One. HAM operators, and presumably interested foreign powers, regularly listen to Air Force One communications.

The Committee recommends the development of strict, rigidly applied communications security practices within the U.S Government if the U.S. is to successfully thwart the active, extensive and often successful electronic espionage conducted every day by the nation's adversaries. The Committee believes that this only will be possible if officials from the President on down make communications security a top priority.

The Committee also recommended that higher priority executive branch attention be given to computer security issues. Vulnerability in this crucial area, where so much of U.S. military and economic superiority is based, could have disastrous results for U.S. national security.

FBI AUGMENTATION

The FBI is in the midst of a program to improve its counterintelligence capabilities and repsond appropriately to the growing counterintelligence threat posed by the presence of foreign espionage agents in the United States. The Committee has fully supported this program and has from time to time augmented it. The Committee is concerned, however, that the pace of FBI personnel increases and other counterintelligence augmentations may require readjustment. In particular, the FBI's surveillance capabilities require improvement and expansion. Several recent espionage cases have pointed to a need for such improvement. While it is difficult to predict a direct correlation between increased counterintelligence capabilities and espionage convictions, throughout its review of recent espionage cases the Committee has been struck by the efforts undertaken by foreign intelligence services to evade FBI surveillance. This suggests that the FBI is effective, but that further improvement is helpful. An investment in better counterintelligence capabilities may be the most cost-effective method of preventing espionage. Clearly also, the statutorily required reduction to Soviet personnel in the United States has helped and will help to reduce the greatest foreign espionage threat of the United States.

The Committee recommends that the Director of Central Intelligence and the FBI Director consider and report to the Congress concerning in the realignment of some FBI surveillance resources to high priority counterintelligence targets as well as the provision of greater emphasis and funds for those counterintelligence techniques which have proven most successful in neutralizing hostile intelligence operations. Another area of possible fruitful investigation would be the development of new opportunities for countering foreign espionage directed at U.S. industrial firms possessing critical technology. The Committee will endeavor to ensure that these capabilities are fully funded in the near future.

On a separate note, the Committee recommends that the Federal Bureau of Investigation initiate a reward program. The FBI could offer a $50,000 reward for providing information leading to the arrest of a foreign intelligence agent attempting to obtain classified

national security information or to the arrest of any government employee or contractor supplying classified information to a foreign power.

CONCLUSION

Any of the weaknesses identified by the Committee, taken alone, would be of concern. What has emerged is a pattern that causes deep dismay about the way U.S. intelligence is managed.

The Committee has also detected faulty hiring practices, poor management of probationary employees, thoughtless firing practices, lax security practices, inadequate interagency cooperation, even bungled surveillance of a prime espionage suspect.

That is a litany of disaster. It leads to concern about the possibility of other undisclosed security vulnerabilities and suggests that the top levels in the U.S. intelligence and the national security communities need to take more aggressive action to improve management regularly and review potential vulnerabilities constantly. Problems that are uncovered should be brought to the attention of appropriate elements of the Congress—with recommendations for statutory changes and new funding, if necessary—and should be promptly reviewed and acted upon.

As a critical first step in this direction, the Committee recommends that the President authorize an independent group of experts outside the intelligence community to examine thoroughly the damage that has been done to U.S. intelligence collection techniques by recent espionage cases, starting with the 1977 convictions of Christopher Boyce and Andrew Dalton Lee. Such a study should analyze what types of intelligence are being denied to the U.S., what steps U.S. adversaries have taken to deny information to the U.S., and what they may be doing to deceive U.S. intelligence as a result of their knowledge of U.S. collection capabilities. That study should recommend steps to adjust and to improve U.S. intelligence collection techniques in this new environment, including any necessary statutory changes. Consistent with security concerns, it should be as widely disseminated as possible so as to combat cynicism and lack of concern about security matters within the national security community. Only by understanding the long term damage of espionage will the nation form the necessary resolve to improve security policies and follow through with the necessary support—financial and otherwise—needed to make a difference.

O